StSchA, IT-BB

An: StSchA, IT-BB
Betreff: AW: RIO-Information: Umgang mit E-Mail-Anhängen mit der Dateiendung „.doc"

Von: ZIT-BB Kundenmanagement
Gesendet: Freitag, 8. November 2019 10:53
An: VL-MIK-RIO-Ausschuss und Vertreter
Cc: Franz, Heiner; LLBB-ITService; Ludwig, Uwe; Ryll, Torsten; ZIT-BB Kundenmanagement; ZIT-BB-Geschäftsstelle-GB1; ZIT-BB-Geschäftsstelle-GB2; ZIT-BB-Geschäftsstelle-GB3; ZIT-BB-Geschäftsstelle-GB4; ZIT-BB-Kaz; ZIT-BB-Öffentlichkeitsarbeit; ZIT-BB-SD
Betreff: RIO-Information: Umgang mit E-Mail-Anhängen mit der Dateiendung ,,.doc"

Sehr geehrte Damen und Herren,

wie Sie den Medien vor einigen Tagen entnehmen konnten, ist das Berliner Kammergericht „Opfer" eines Cyberangriffs geworden. Die Angreifer haben dabei Schadcode in ,,.doc-Dateianhängen" versteckt, die beim Öffnen des Dokumentes/Anhangs automatisch ausgeführt werden. Das ,,.doc"-Format von Microsoft ist ein veraltetes Dateiformat, das aktuell von Hackern missbraucht wird, um Schadcode zu verteilen.

Der Großteil von Cyberangriffen auf die öffentliche Verwaltung in Brandenburg wird über verschiedene Stufen und Virenscanner herausgefiltert. Da der Schadcode von den Angreifern einer stetigen Anpassung unterliegt, um unerkannt zu bleiben, können nicht immer alle infizierten E-Mail-Anhänge von den Filtersystemen erkannt werden. Dies insbesondere dann nicht, wenn die Hersteller der Virenschutzsoftware noch nicht von den Änderungen der Angreifer Kenntnis haben und ihre Virenscanner somit noch nicht anpassen konnten.
In solchen Fällen erreichen infizierte E-Mail-Anhänge den Benutzer/die Benutzerin und können erheblichen Schaden an der IT-Infrastruktur des Landes anrichten. Ist der Computer erst infiziert, lädt er oft (wie im Fall „Emotet") weitere Schadsoftware nach und verteilt diese weiter im IT-Netz. In mehreren dem BSI bekannten Fällen hatte dies große Ausfälle der IT-Infrastruktur zur Folge, da ganze Netzwerke neu aufgebaut werden mussten (z.B. auch das Netz des Deutschen Bundestages).
Aktuell werden in Spitzenzeiten täglich bis zu 1.000 Cyberangriffe an den Netzübergängen beim zentralen IT-Dienstleister des Landes Brandenburg (ZIT-BB) registriert. Um auch zukünftig sicher gegen veränderte Schadcode-Versionen, die über das alte Microsoft Office ,,.doc"-Format eingeschleust werden könnten, gewappnet zu sein, hat das Informationssicherheits-Managementteam (ISMT) der Landesverwaltung Brandenburg am 16.10.2019 den ZIT-BB beauftragt, eine generelle Filterung dieser E-Mails/Anhänge vorzunehmen.

Die IT-Sicherheitsmaßnahme wird am zentralen E-Mail-Eingang des Landesverwaltungsnetzes (LVN) implementiert und betrifft auch Ihre Organisation, soweit Ihre Email-Kommunikation über diesen E-Mail-Eingang läuft. Die Filterung hat folgende Konsequenzen:

Die technisch mögliche Filterung sieht die unwiderrufliche Löschung der eingehenden E-Mails vor, die einen Anhang aufweisen, der eine Datei im alten ,,.doc"-Format beinhaltet. Der Empfänger erhält lediglich die Meta-Daten der ursprünglichen Email/Nachricht mit dem Hinweis, dass die E-Mail wegen eines unerlaubten Anhangs verworfen wurde. Dadurch erhält der Empfänger die Möglichkeit ggf. dem Absender darüber zu informieren und zu bitten, entsprechend der gültigen Landesstandards z.B. nur pdf-Dokumente ihm einzusenden. Der E-Mail-Absender erhält indessen keine Information darüber, dass die von ihm versendete E-Mail den Empfänger nicht in der verschickten Form erreicht hat. Durch die Rückmeldungsmöglichkeit des Empfängers wird der notwendige Informations- bzw. Datenaustausch letztlich aber auch weiterhin gewährleistet.

Vor dem Hintergrund der bestehenden Bedrohungslage wurde ab der 44. KW ein ZIT-BB-interner Test durchgeführt, eine Aktivierung der Filterung ist ab der KW 46 vorgesehen. Ich bitte um Ihr Verständnis für das beschriebene Vorgehen. Für Rückfragen steht Ihnen der ZIT-BB gerne zur Verfügung.

Freundliche Grüße
Im Auftrag

Ihr Kundenmanagement
Brandenburgischer IT-Dienstleister
Adresse: 14480 Potsdam, Steinstraße 104-106
Telefon: +49 331 39-1198
Fax: +49 331 398-1198
E-Mail: km@zit-bb.brandenburg.de
Internet: https://.zit-bb.brandenburg.de
